12 FAM 650
ACQUISITION SECURITY REQUIREMENTS FOR OPERATING SYSTEMS AND SUBSYSTEM COMPONENTS

(TL:DS-51; 04-12-1996)

12 FAM 651 GENERAL

(TL:DS-51; 04-12-1996)

a. Acquisition authorities must follow these security requirements when purchasing operating systems and add-on subsystem security components.

b. Exceptions to this subchapter must be justified in accordance with operational resource implications. Such exception requests must be submitted in writing and outline both the resource implications and the projected timeframe of the bureau or office to comply with this subchapter. Requests for exceptions will be considered by DS/CIS, in consultation with DS/CIS/IST.

c. Automated information systems (AISs) that process classified intelligence information must meet the requirements set forth in the Director of Central Intelligence Directive 1/16, "Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks (July 19, 1988)."

12 FAM 652 CLASSIFIED AND UNCLASSIFIED AUTOMATED INFORMATION SYSTEMS OPERATING IN THE SYSTEM HIGH MODE

12 FAM 652.1 Level of Trust for Operating Systems and Subsystem Components Processing Classified Information

(TL:DS-51; 04-12-1996)

a. DS/CIS/IST requires that system and subsystem acquisition authorities select C2 rated products listed in the National Security Agency's

Evaluated Products List (EPL) contained in the Information Systems Security Product and Services Catalogue for classified processing in the system high mode.

Note: National Telecommunications and Information System Security Policy 200 (NTISSP 200) entitled "National Policy on Controlled Access Protection" requires the C2 level of protection described in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), dated December 1985. This document specifies that C2 class systems provide controlled access protection for all information on the Automated Information System (AIS) and requires identification and authentication, auditing of security relevant events, discretionary access controls, and object reuse.

b. If the use of EPL products is not feasible, or if the product selected has not completed a full evaluation, the acquisition authority must contact DS/CIS/IST. DS/CIS/IST may forgo the requirement for rated products and allow system acquisition authorities to purchase the selected product after consultation with the National Security Agency's Security Profiling and Trusted Products Evaluation Program (TPEP) organizations.

c. DS/CIS/IST will accept security subsystems for use in personal computers that meet security requirements for identification and authentication, discretionary access controls, auditing, and object reuse in lieu of the aforementioned C2 requirements. System and subsystem acquisition authorities must ensure that all PCs are equipped with a security subsystem if the features of Class C2 are not otherwise present.

Note: Subsystem EPL entries are rated based on TCSEC Evaluation Criteria Class D. Class D has been reserved for products that do not meet the specified requirements for that of a higher evaluation criteria class. Subsystem components are special-purpose add-on security products that introduce specific security features (i.e., identification and authentication, discretionary access control, audit, and object reuse.)

12 FAM 652.2 Level of Trust for Operating Systems and Subsystem Components Processing Unclassified Information

(TL:DS-51; 04-12-1996)

DS/CIS/IST requires that system and subsystem acquisition authorities select products that provide automated controlled access protection for unclassified processing in the system high mode. Personal computers must be equipped with security subsystems as described in section 12 FAM 652., paragraph c.

12 FAM 652.3 Requirements for Unclassified and

Classified Automated Information Systems

12 FAM 652.3-1 General

(TL:DS-51; 04-12-1996)

a. The acquisition authority must ensure that operating systems selected for use on Department of State automated information systems meet the following requirements.

b. Security subsystems must conform to these operating system and subsystem requirements to the extent possible.

12 FAM 652.3-2 Discretionary Access Controls

(TL:DS-51; 04-12-1996)

The following requirements are based upon the National Computer Security Center's "Guide to Understanding Discretionary Access Controls in Trusted Systems":

(1) AISs must have the capability to restrict access privileges. Users will be assigned one of the three different access privileges below:

(a) System security administrators;

(b) Operators; or

(c) General users;

(2) AISs must be able to restrict users from access to terminals and printers on an individual basis;

(3) Providing the capability exists, an AIS must automatically disconnect terminals after "n" minutes of inactivity. The inactivity duration may only be set by the system security administrator who will balance operational and security needs in choosing a time period;

(4) AISs must have the capability to logically disconnect any terminal at the discretion of the system security administrator or operator;

(5) AIS initial program loads or power ups must result in reinitialization of the interfaces to all logically connected devices. The power up of a peripheral will reinitialize the peripheral;

(6) AIS must be able to limit the number of unsuccessful logon attempts through a lock-out capability. Powering an AIS up or down must not affect the lockout status. The capability to reactivate locked-out terminals must be restricted to the system security administrator;

(7) AISs must require a user profile for each user. Such profiles will be

used to mediate access to named objects (e.g., files, programs);

(8) The capability to establish and modify user profiles must be restricted to the system security administrator.

12 FAM 652.3-3 Identification and Authentication

(TL:DS-51; 04-12-1996)

The following requirements are based upon the National Computer Security Center's "Guide to Understanding Identification and Authentication in Trusted Systems":

(1) AIS must require entry of a three character (minimum) user identification string for all AIS users;

(2) AISs must require entry of a six to eight character password, consisting of a combination of alphabetic and numeric characters, to authenticate a user's identity. In addition to alpha-numerics, the password may include punctuation marks, mathematical characters and other traditional characters.

12 FAM 652.3-4 Audit

(TL:DS-51; 04-12-1996)

The following requirements are based upon the National Computer Security Center's "Guide to Understanding Audit in Trusted Systems":

(1) An AIS must have the capability to audit the following events:

(a) Use of identification and authentication mechanisms (i.e., system login);

(b) Introduction of objects into a user's address space (e.g., fopen, file creation, program execution, fcopy);

(c) Deletion of objects from a user's address space (e.g., fclose, completion of program execution, file deletion);

(d) Actions taken by computer operators and system administrators and/or system security administrators (e.g., adding a user);

(e) Security-relevant events (e.g., use of privileges, changes to DAC parameters); and

(f) Production of printed output;

(2) AISs must be able to record the following information about auditable events:

(a) Dates and times of event;

(b) User or process identification;

(c) Type of event (one of the events named above);

(d) Success or failure of events;

(e) Origin of the request (i.e., terminal identifier); and

(f) Name of the object involved (e.g., file being deleted);

(3) AISs must ensure the audit trail configuration capability is available only to the system security administrator;

(4) The system shall automatically provide notification to the system operator or administrator when the audit trail medium is approaching its allocated storage capacity (approximately 80% full);

(5) Audit data reduction tools shall be provided for the use of the security administrator which extract subsets of audit data for individual analysis.

12 FAM 652.3-5 Object Reuse

(TL:DS-51; 04-12-1996)

The following requirements for C2 rated operating systems are based upon the National Computer Security Center's, "A Guide to Understanding Object Reuse in Trusted Systems." They should be implemented to the extent possible:

(1) The AIS will protect unauthorized disclosure of information contained in the AISs storage objects;

(2) Each individual register and storage object must be initialized before the space is allocated to a user;

(3) If the storage object is not immediately initialized once the information has been released (e.g., copied, moved, deleted), the AIS must maintain adequate protection of that storage object and any information contained within.

12 FAM 652.3-6 Top Secret Control

(TL:DS-51; 04-12-1996)

The requirements of this section are applicable only if the system is utilized to process objects classified Top Secret:

(1) The system shall have the capability to record access to all Top Secret data objects by named users as an event and to maintain audit information pertaining to such events;

(2) Records of the following information are to be maintained:

(a) Date and time of the event;

(b) User identification;

(c) User's physical system;

(d) Type of access (e.g., read only, copy, append, or write access);

(e) Top Secret Control Number;

(f) Success or failure of the event;

(g) Origin of the request; and

(h) Name of the object.

12 FAM 653 CLASSIFIED AND UNCLASSIFIED AIS NETWORKS OPERATING IN THE SYSTEM HIGH MODE

(TL:DS-51; 04-12-1996)

Classified and unclassified AIS networks operating in the system high mode must adhere to minimum functional system and network security requirements.

12 FAM 653.1 Discretionary Access Controls

(TL:DS-51; 04-12-1996)

a. The local AIS access control mechanism must validate the intended recipient's access authorization.

b. The local AIS must require users to assign a sensitivity attribute concerning message classification prior to data transmission.

c. Networked AISs must be capable of maintaining storage objects received from other AISs so they are accessible only to authorized recipients and the system security administrator.

12 FAM 653.2 Authentication

(TL:DS-51; 04-12-1996)

Networked AISs must ensure data exchanges are established only with addressed entities.

12 FAM 653.3 Communications Integrity

(TL:DS-51; 04-12-1996)

a. Networked AISs must protect communication protocols and data fields from unauthorized modification.

b. Networked AISs must ensure information is accurately transmitted from the source to the destination.

c. Networked AISs must have an automated capability to test for, detect, and report errors that exceed the network's defined thresholds on central processing unit (CPU) usage, disk utilization, or when task activities are exceeded.

d. Networked AISs transiting non-USG controlled space must employ U.S. Government approved data modification countermeasures, such as digital signatures, authentication codes, encryption techniques, etc., to reduce the vulnerability to the threat of illegal or unauthorized access.

12 FAM 653.4 Continuity of Operations

(TL:DS-51; 04-12-1996)

a. Networked AISs must have utilities capable of monitoring AIS performance and alerting the system manager to possible denial of service conditions. Denial of service conditions include system flaws that would allow an unauthorized user to defeat DAC or that would cause the TCB to enter a state in which it's unable to respond to user requests.

b. Networks must provide redundant control capabilities that will sufficiently reduce single points of failure, enhance reliability and survivability, and provide excess capacity. For example, the system manager may define a primary and secondary transmission path between systems within the network.

12 FAM 653.5 Protocol-Based Protection Mechanism

(TL:DS-51; 04-12-1996)

Networked AISs must employ protocol-based mechanisms to minimize the potential for equipment crashes and deadlocks. The AIS should be capable of detecting network problems (e.g., slowdown in transmission) using existing protocol services. One technique could require measurement of transmission rates between systems (compare with minimum) and waiting time for responses (compare with threshold).

12 FAM 653.6 Data Confidentiality

(TL:DS-51; 04-12-1996)

a. Networked AISs must protect data from unauthorized disclosure during storage and transmission.

b. Classified networks must use equipment approved by the National Security Agency to achieve end-to-end data encryption when transmitting outside secure areas.

c. Classified AISs may use protected distribution systems or the equivalent security controls when transmitting within a secured area. Note: DTS/1A contains additional information.

d. Classified AISs must address the implementation of countermeasures to prevent data disclosure through compromising emanations (TEMPEST). Note: Additional guidance is contained in National Telecommunications and Information System Security Policy 300 (NTISSP 300) entitled "National Policy on Control of Compromising Emanations."

e. Classified networks must implement communications security procedures per subchapter 12 FAM 660 .

12 FAM 653.7 Traffic Confidentiality

(TL:DS-51; 04-12-1996)

a. Classified networks must conceal origin and destination patterns for communications between protocol entities (e.g., encryption).

b. Classified networks must have the capability to disguise traffic levels.

12 FAM 653.8 Top Secret Control

(TL:DS-51; 04-12-1996)

The requirements of this section are applicable only if the network is utilized to process classified Top Secret information:

(1) The receiving system shall have the capability to report the successful receipt of (transmitted) Top Secret messages or objects to the sending system;

(2) Verification of the successful receipt of the (transmitted) Top Secret data object by the destination system shall be recorded with other system accountability data such that it is protected from modification or unauthorized access or destruction. The destination system and the Top Secret control number shall be recorded with other required audit data.

12 FAM 654 THROUGH 659 UNASSIGNED